In The Claims:

Please cancel without prejudice claim 16.

Please amend the remaining claims as follows:

1. (currently amended) A disk drive comprising:

(a) a disk for storing data, the disk comprising a public area for storing plaintext data and a pristine area for storing encrypted data;

(b) a head for reading the encrypted data from the pristine area of the disk;

~~(d)~~(c) a control system for interfacing with a host computer to ~~controlling access to the~~facilitate read and write commands to write data to and read data from the pristine area of the disk, the control system comprising:

authentication circuitry for authenticating a request received from ~~an external entity~~the host computer to access the pristine area of the disk ~~and for enabling the control system if the request is authenticated~~;

~~(e)~~a secret drive key; and

~~(f)~~decryption circuitry, responsive to the secret drive key, for decrypting the encrypted data stored in the pristine area of the disk to generate decrypted data.

2. (original) The disk drive of claim 1, wherein the encrypted data comprises encrypted authentication data.

3. (original) The disk drive of claim 2, wherein the authentication circuitry is responsive to the decrypted data.

4. (original) The disk drive of claim 2, wherein the encrypted authentication data comprises encrypted user authentication data.

5. (original) The disk drive of claim 2, wherein the encrypted authentication data comprises encrypted device authentication data for authenticating a device, the device comprising a unique device ID configured during manufacture of the device.

6. (original) The disk drive of claim 2, wherein the encrypted authentication data comprises encrypted information for implementing a challenge and response verification sequence.

7. (original) The disk drive of claim 2, wherein the encrypted authentication data comprises encrypted message authentication data.

8. (original) The disk drive of claim 7, wherein the encrypted authentication data comprises encrypted key data for generating a message authentication code.

9. (original) The disk drive of claim 1, wherein the encrypted data comprises encrypted key data for decrypting an encrypted message.

10. (original) The disk drive of claim 1, wherein the encrypted data comprises encrypted message data.

11. (original) The disk drive of claim 1, wherein the disk drive further comprises encryption circuitry for encrypting plaintext data into the encrypted data stored in the pristine area.

12. (original) The disk drive of claim 1, wherein:
(a) the disk further comprises embedded servo sectors comprising servo bursts;
(b) the control system comprises a servo control system responsive to the embedded servo sectors; and
(c) the authentication circuitry enables the servo control system.

13. (original) The disk drive of claim 12, wherein:

(a) the servo bursts are written to the disk in encrypted form; and

(b) the authentication circuitry enables the servo control system to decrypt the servo bursts.

14. (original) The disk drive of claim 13, wherein:

(a) the servo bursts are written to the disk with additive noise generated from a pseudo random sequence;

(b) the pseudo random sequence is generated from a polynomial;

(c) the servo control system uses the polynomial to decrypt the servo bursts; and

(d) the authentication circuitry provides the polynomial to the servo control system.

15. (canceled)

16. (canceled)

17. (currently amended) A method of processing a request received by a disk drive from ~~an external entity~~ a host computer to access encrypted data stored in a pristine area of a disk, the method comprising the steps of:

(a) using a control system internal to the disk drive to receive the request from the host computer;

~~(a)~~(b) using the control system internal to the disk drive to authenticate~~ing~~ the request to access the pristine area and ~~enabling~~ to enable access to the pristine area if the request is authenticated;

~~(b)~~(c) using the control system internal to the disk drive to ~~reading~~ read the encrypted data stored in the pristine area; and

~~(c)~~(d) using the control system internal to the disk drive to ~~decrypting~~ decrypt the encrypted data using a secret drive key within the disk drive to generate decrypted data.

18. (original) The method as recited in claim 17, wherein the encrypted data comprises encrypted authentication data.

19. (original) The method as recited in claim 18, wherein the step of authenticating is responsive to the decrypted data.

20. (original) The method as recited in claim 18, wherein the encrypted authentication data comprises encrypted user authentication data.

21. (original) The method as recited in claim 18, wherein the encrypted authentication data comprises encrypted device authentication data for authenticating a device, the device comprising a unique device ID configured during manufacture of the device.

22. (original) The method as recited in claim 18, wherein the encrypted authentication data comprises encrypted information for implementing a challenge and response verification sequence.

23. (original) The method as recited in claim 18, wherein the encrypted authentication data comprises encrypted message authentication data.

24. (original) The method as recited in claim 23, wherein the encrypted authentication data comprises encrypted key data for generating a message authentication code.

25. (original) The method as recited in claim 17, wherein the encrypted data comprises encrypted key data for decrypting an encrypted message.

26. (original) The method as recited in claim 17, wherein the encrypted data comprises encrypted message data.

27. (original) The method as recited in claim 17, further comprising the step of encrypting plaintext data to generate the encrypted data stored in the pristine area.

28. (original) The method as recited in claim 17, wherein the disk further comprises embedded servo sectors comprising servo bursts, the method further comprising the steps of:

(a) servoing a head over the disk in response to the embedded servo sectors; and

(b) enabling servoing in the pristine area if the request is authenticated.

29. (previously presented) The method as recited in claim 28, wherein:

(a) the servo bursts are written to the disk in encrypted form; and

(b) the step of authenticating the request to access the pristine area comprises the step of decrypting the servo bursts.

30. (previously presented) The method as recited in claim 29, wherein:

(a) the servo bursts are written to the disk with additive noise generated from a pseudo random sequence;

(b) the pseudo random sequence is generated from a polynomial; and

(c) the step of servoing uses the polynomial to decrypt the servo bursts.

31. (currently amended) A method of processing a request received by a disk drive from ~~an external entity~~a host computer to access data stored on a disk, the disk comprising a public area for storing plaintext data and a pristine area for storing encrypted data, the method comprising the steps of:

(a) using a control system internal to the disk drive to receive the request from the host computer;

~~(a)~~(b) using the control system internal to the disk drive to ~~decrypting~~ decrypt the encrypted data stored in the pristine area of the disk using a secret drive key within the disk drive to generate decrypted data; and

~~(b)~~(c) using the control system internal to the disk drive to ~~using~~ process the decrypted data to authenticate the request received from the ~~external entity~~host computer before allowing access to the disk.

Please add the following new claim:

32. (new) A disk drive comprising a disk for storing data, and a head for reading data from the disk, the improvement comprising:

a control system for interfacing with a host computer to facilitate read and write commands to write data to and read data from the disk, the control system comprising:

authentication circuitry for authenticating a request received from the host computer to access the disk;

a secret drive key; and

decryption circuitry, responsive to the secret drive key, for decrypting the encrypted data stored on the disk to generate decrypted data.